CYBERSECURITY REQUIREMENTS

Type 3 Contracts

TABLE OF CONTENTS

PREAMBLE

The following Cybersecurity Requirements set the minimum and standard framework of the requirements that must be met by the Supplier and its Subcontractors in the performance of Type 3 Contracts. Type 3 (non-technical) purchases are defined as contractual engagements where there is no direct access or interface connection with TotalEnergies' systems or data.

Additional requirements must be satisfied for higher risk engagements involving direct access or interface with TTE network systems, defined as Type 1 & 2 contracts, and those will be attached to the relevant contract.

Cybersecurity Requirements shall not prevail over or defeat the application of (i) applicable laws and regulations relating to the Cybersecurity of Systems and data; (ii) more precise and stringent applicable rules relating to the Cybersecurity of Systems and Data, such as certifications to standards (such as ISO, ETSI or European Cybersecurity) applicable to the Supplier, its products, procedures, and/or services; (iii) the Customer's Internal Rules; and (iv) the requirements otherwise agreed by the Parties.

Certain Information Systems and their Resources, due to their sensitivity, may be subject to regulations, in particular in terms of confidentiality (e.g., defense secrecy), technical, human and organizational obligations, control and audit, qualification and accreditation, alert and crisis management, etc. Specific Internal Rules (including the Information Systems Security Policy) as well as specific contractual rules will also apply and prevail over these Cybersecurity Requirements.

Regarding AI Technologies, additional mandatory procedures and provisions will apply when these technologies are intended to be used within critical infrastructures or sensitive or vital systems and networks of the Customer, or those systems and networks subject to specific cybersecurity regulations. The same will apply to all high-risk AI systems. The stipulations in these AI requirements cannot replace or apply by default to such cases.

References to the Supplier must be understood as including the Supplier and its Subcontractors, the Supplier's obligations extending to the Information Systems and Resources of its Subcontractors.

TERMS AND DEFINITIONS

The terms defined below apply only to security requirements – they may in no way be used as a reference in the other contractual documents of the Contract.

AI Technology: Any artificial intelligence model or system incorporated, used, and/or operated under the Contract and falling within the scope of applicable regulations including but not limited to Regulation (EU) 2024/1689 ("AI Act") and the Texas Responsible Artificial Intelligence Governance Act ("TRAIGA").

Audit: Set of checks to ensure the compliance of the Supplier, its services, or goods with its legal and contractual obligations in terms of Cybersecurity. Types of Audits: organizational, compliance, configuration, and technical (intrusion, code review, etc.).

Authentication: A method of verifying the identity of a user accessing the Information System.

CERT (Computer Emergency Response Team) TotalEnergies: The IT emergency response team responsible for coordinating incident response and Cybersecurity assessment for TotalEnergies entities and their respective Suppliers. See https://totalenergies.com/cert

Classification: The classification of a Resource by the Customer provides the Supplier with a concise indication of its importance and the need for an appropriate level of protection for the Resource.

Classification Profile: The classification profile of a Resource is an assigned value that corresponds to the potential impact of the Risks likely to affect the Resource, analyzed according to the three criteria considered. Each Resource is therefore assigned, for each of the Availability, Integrity and Confidentiality criteria, a sensitivity level (0=Low impact level to 4=High impact level).

Contract: Refers to all the documents governing the contractual relationship between the Supplier and the Customer for a defined service.

Contract-Specific Resources: Includes Resources under the responsibility of the Supplier and its Subcontractors that are implemented specifically for the Contract – (including, in particular, the workstations of the employees involved in the Contract and the Resources that are used in the performance of the Contract).

Customer Data: Data (including personal data) to which the Supplier has access under the Contract and the data generated by the Systems (including logs and metadata).

Cybersecurity: All the technical and organizational measures that are necessary for and proportionate to the protection of the Customer's Information Systems and Resources, the Contract-Specific Resources, Customer Data, users and third parties that could be impacted, against events or actions likely to compromise the availability, authenticity, integrity, or confidentiality of the Information Systems and Resources, the Customer Data, and/or the services to be performed.

Cybersecurity Incident: Any Event that is likely to call into question the Cybersecurity or the normal functioning of a Resource of the Information System (or a service provided by the IS function) of the Customer or any Contract-Specific Resources and likely to affect the availability, the integrity, or confidentiality of the relevant Resource or Customer Data.

Enterprise Information Systems (EIS): Information Systems comprising services and applications intended for business management (office automation, human resources, customer relations, finance, treasury, purchasing, etc.).

Event: Information generated by a component of the Information System that is recorded in a log.

Industrial Information Systems (IIS): Information Systems comprising Systems and components that contribute directly to the production processes, integrity, safety, and security of sites (command control systems, laboratory management Systems, technical management Systems, etc.).

Information System (IS): An organized set of Resources for processing data and providing services. The Information System is essential to the Customer's activities under the Contract. It includes the Enterprise Information System and the Industrial Information System.

Internal Rules: Customer's internal rules and procedures specific to the Information System(s) or the Customer's sites that are transmitted by the Customer to the Supplier or that are accessible from the Customer's intranet.

Major Cybersecurity Incident: Any Cybersecurity Incident with potentially major consequences according, if applicable, to the levels indicated in the Security Assurance Plan.

Malicious Code: Any program developed for the purpose of harming a computer System or a network.

(Cybersecurity) Measure: Those means that are taken to manage a risk. The means may be of an administrative, technical, managerial, or legal nature (including, in particular, the policy, procedures, guidelines, and organizational practices or structures of the Systems).

Privileged Access: Authorization to access a Resource to perform resource administration operations (e.g. read the configuration, modify the configuration, execute a command reserved for an administrator, delete files, etc.).

Remediation: Implementation of security means or measures to resolve errors, flaws, defects, or failures in Cybersecurity.

Resource (of the Information System): All or part of the means, services, and processes involved in the operation of the Customer Information System, such as, in particular, applications, data, technical means, equipment, and networks (local, corporate, etc.). Resources include those means, services, and processes of the Suppliers that impact or involve the Customer's Information System – including, for example, Cloud or SaaS service providers, service providers in charge of managed or outsourced services, etc.

(Cybersecurity) Risk: A Risk characterized by:

- a threat or malicious action of internal or external origin on Information Systems.
- a threat or non-malicious action, such as a failure, negligence, or error of the Information Systems.

Security Committee (SECCO): Decision-making and monitoring body for action plans and Cybersecurity indicators.

Security Assurance Plan (SAP): Document describing the terms of performance of the Contract from a Cybersecurity point of view. This document describes the Cybersecurity indicators, the Cybersecurity organization, and the specific Cybersecurity Measures put in place.

Security Operation Center (SOC): A centralized function within an organization that employs people, processes, and technologies to continuously monitor and improve the organization's security posture while preventing, detecting, analyzing, and responding to Cybersecurity Incidents.

State of the Art: Principles and fundamental notions of the security of Information Systems – including, in particular, those described in standards (ISO, IEC) and texts published by official bodies (ANSSI, NIST, ENISA).

Strong Authentication: Authentication based on at least 2 of the following:

- a secret known to the user only (password, PIN);
- an object owned by the user (card generating one-time passwords, smart card, USB key);
- a physical characteristic of the user (fingerprint, retinal fingerprint, hand structure, or any other biometric element).

Systems: The Information Systems of the Customer or the Supplier used in the context of the Contract.

(Cybersecurity) Threat: Potential cause of a Cybersecurity Risk which can harm an Information System or an organization.

Vulnerability Levels: The CERT defines and specifies the levels of vulnerability (e.g. P0, P1, Standard). These levels are included in the Security Assurance Plan if applicable.

Requirements for Type 3 Contracts

1. Raise awareness of Cybersecurity among personnel	Cybersecurity Awareness and Training

The Supplier must conduct awareness-raising actions among the personnel involved in the performance of the Contract (including Subcontractors) to ensure that they are aware of the Cybersecurity rules to be applied.

2. Manage Incidents related to Malicious Codes	Protection against malicious code

The Supplier must define and implement processes and procedures for managing Threats and Malicious Codes. The Supplier is required to comply with its contractual and legal obligations to timely report Cybersecurity Incidents to the Customer - including the breach of personal or non-personal data.

3. Secure the mobile devices used for the Contract	Security of mobile systems, workstations, and equipment

The Supplier must ensure the existence of specific and appropriate Measures for the security of its mobile devices (all types of connected equipment) used by its personnel (and/or those of its Subcontractors) to be used in the performance of the Contract and ensure the use of these Measures by its personnel and its Subcontractors in the performance of the Contract.

4. Secure the digital media used for the Contract	Security of Digital media

The Supplier must put in place adequate Measures to protect the digital media on which the Customer Data resulting from the performance of the Contract is copied, saved, and/or archived.
Supplier's computer media used in the performance of the Contract must be subject to a formalized Classification and must be in line with the type of data copied, backed up, and/or archived.
The inventory of Supplier's computer media must be available and kept up to date. Backup and computer archiving media must be secured and protected on an ongoing basis against illegal acts and environmental risks. The transport of computer media must be subject to a documented procedure.

5. Alert in case of a Major Security Incident	Cybersecurity Incident Management

Major Cybersecurity Incident must be reported to the CERT TotalEnergies within four (4) hours from the moment the Supplier becomes aware of it. Each report must specify, in particular, the nature and extent of the Major Cybersecurity Incident (proven and potential) and contain information to enable the Customer to assess the consequences for itself. The Supplier must actively collaborate with the Customer on each Cybersecurity Incident and regularly update this information.

6. Respond to requests from a crisis unit of the Customer	Cybersecurity Incident Management

The Supplier must have a crisis management organization that allows the Supplier to respond to requests from the Customer's crisis unit as soon as possible.

7. Test the continuity of business related to the Contract	Business Continuity Requirements

The Supplier must carry out systematic tests of its organizational, human, and technical solutions for ensuring business continuity and disaster recovery. These tests must be conducted at the end of their development by the Supplier and supplemented by tests and regular exercises to evaluate the functioning of all the continuity and disaster recovery plans that it has defined.

8. Favor the use of collaborative tools	Collaborative tools & shared Workspaces

In its exchanges with the Customer, the Supplier must use, as far as possible, the collaborative work tools suggested or made available to it by the Customer. In certain cases (in particular, cases requiring confidentiality) the Supplier will be obliged to use the collaborative work tools of the Customer.

9. Delete e-mail messages and documents related to the Contract at the end of the Contract	Collaborative tools & share Workspaces

Within a maximum period of one month from the termination of the Contract for any reason whatsoever, the Supplier must delete from its own Resources all Contract-Specific Resources, Customer Data, and electronic messages and documents except to the extent (a) otherwise stipulated in a contractual document that takes precedence over these requirements; (b) there is a mandatory legal obligation for retention; (c) retention is needed for the purposes of certifying the product or service that is the subject of the Contract; and/or (d) retention is specifically agreed between the Parties at the termination of the Contract.

10. Comply with rules governing messaging and collaborative tools	Collaborative tools & shared Workspaces

The Supplier must comply with State of the Art rules of good practice associated with messaging and collaborative tools provided to it by the Customer.

11. Declare AI Technologies Used in the Contract	Knowledge of AI Technologies

Before any use of AI Technologies in connection with the Contract, the Supplier must declare in writing to the Customer the AI Technologies it wishes to use in connection with the Contract - from the signing of the Contract throughout the duration of the performance of the Contract. For the entire duration of the Contract, the same applies in case of any modifications to or changes in the AI Technologies used in connection with the Contract.

The Customer may oppose in writing the use of AI Technologies without having to justify and without compensation or indemnification to the Supplier. The AI Technologies initially agreed shall continue through the duration of the Contract.

The AI Technologies authorized on the day of the signing of the Contract shall be exhaustively specified in the Description of Services Schedule of the Contract.

12. Compliance of AI Technologies Used in the Contract	Compliance of AI Technologies

The Supplier warrants (for itself and its Subcontractors) that the AI Technologies to be used in connection with the Contract:
Do not include any AI prohibited under any applicable laws and that no prohibited AI has been previously used in relation to the AI Technologies to be used in connection with the Contract;
Do not include high-risk AI, except (a) with the prior written consent of the Customer and (b) subject to the application of specific and prior procedures, and contractual and technical conditions provided for by applicable laws;
Comply, within any applicable legal deadlines, with all applicable laws and are updated according to changes in applicable laws at no additional cost to the Customer;
Have not been subject, in the last six (6) months, to interruptions resulting from the use of any emergency mechanism to prevent the AI technologies from executing or performing a particular function;

Are implemented within the framework of strict specifications, design, and control and supervision protocols to restrict access to (a) the AI Technologies to be used in connection with the Contract and (b) training, testing, verification, and improvement data; and

There has been no unauthorized access to (a) the algorithm or software incorporating the AI Technologies to be used in connection with the Contract or (b) the training, testing, and verification data used to (i) train personnel working on the Contract and/or (ii) improve the AI Technologies to be used in connection with the Contract.

13. Monitor Operations Performed on AI Technologies	Compliance with Obligations on AI Technologies

The Supplier shall:

- Provide the Customer with all technical and functional documentation regarding the AI Technologies to be used in connection with the Contract.
- Implement all obligations defined in applicable laws – particularly, quality assurance measures, risk management, human oversight, information, and transparency.
- Keep information that explains the operations carried out, the results produced, and the decisions made or facilitated by the AI Technologies to be used in connection with the Contract in a readable and easily accessible form for the Customer or regulatory authorities.